

09/463907

Serial No.

To be assigned

Atty Docket
162/547

Applicant

420 Recd PCT/PTO 02 FEB 2000

Shiho Moriai et al.

Filing Date
HerewithGroup Art Unit
To be assigned

FORM PTO-1449

INFORMATION DISCLOSURE CITATIONU.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub-Class	Trans-lation
	AL						Yes No
	AM						Yes No

OTHER (Including Author, Title, Date, Pertinent Pages, etc.)

<i>SH</i>	AN	Shiho Moriai, "How to Design Secure S-boxes against Differential, Linear, Higher Order Differential, and Interpolation Attacks," Telecommunications Advancement Organization of Japan, SCIS '98, 2.2C, January 1998, pp. 1-8
<i>SH</i>	AO	Hamade, Takeshi, et al., "On Partitioning Cryptanalysis of DES," Telecommunications Advancement Organization of Japan, SCIS '98, 2.2A, January 1998, pp. 1-8
<i>SH</i>	AP	Langford, S.K., and Hellman, M.E., "Differential-Linear Cryptanalysis," Lecture Notes in Computer Science, Advances in Cryptology CRYPTO '94, Vol. 839, 1994, pp. 17-25
<i>SH</i>	AQ	Sakurai, Kouichi, "Angou riron no kiso," Kyoritsu Shuppan, pp. 69-72, 1996
<i>SH</i>	AR	Kanda, Masayuki, et al., "A Round Function Structure Consisting of Few S-boxes (Part II)," Telecommunications Advancement Organization of Japan, SCIS '98, 2.2.D, January 1998, pp. 1-8
<i>SH</i>	AS	Moriai, Shiho, et al., "S-box Design Considering the Security Against Known Attacks on Block Ciphers," Technical Report of the IEICE, ISEC98-13, Vol. 98, NO. 227, 30 July 1998, pp. 25-32

Examiner

Date Considered

11/16/06

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP § 609.

Draw line through citation if not in conformance and not considered.

Include copy of this form with next communication to Applicant.